I/UCRC: CARFS
Center for Advanced Research in Forensic Science

Investigating Methods to Capture Guest VM Memory

PI: Dr. Jordan Shropshire

IST / School of Computing

UNIVERSITY OF SOUTH ALABAMA

DFII: Digital Forensics Information Intelligence

RELEVANCE / OBJECTIVES

Relevance

- Results in techniques and tooling to support live observation and analysis of virtual machine memory
- Purpose is to detect malicious code executing within the VM
- This project would provide a out-of-band method for observing guest VM memory
- The proposed approach renders memory outputs which are formatted for rapid analysis.
- Depictions are analyzed using a pattern recognition algorithm.

APPROACH / TECHNIQUES

- VM memory is observed from a peering point within the hypervisor.
  - No software is installed within the guest operating system
  - No writes to guest memory are required
- Creates accurate guest-to-metal memory map
  - Introspects guest to support memory mapping
  - Observe mappings between guest virtual memory and guest physical memory
- Minimizes smear by manipulating the hypervisor scheduler
  - Temporarily degrades VM performance via credit scheduling algorithm

MILESTONES / DELIVERABLES

Deliverables

- Developing tooling to support smart VM memory analysis
- Design for integration with Xen platform

Milestones

- 4 m: Incorporate existing code for passive introspection
  Standardized format for outputting VM memory
- 8 m: Develop methods for mapping guest virtual memory to host virtual memory
- 12 m: Assemble near-real-time mapping between guest virtual memory and host physical memory
  Create tooling to identify and extract guest physical memory

INDUSTRY BENEFITS

Economics

- Provides an efficient method of analyzing suspicious VMs
- Minimize the risk of undiscovered malware

Potential Member Benefits

- Saves time and effort in extracting and analyzing VM memory
- Automates much of the workflow